REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed March 7, 2008. Upon entry of the amendments in this response, claims 1 – 46 remain pending. In particular, Applicants amend claims 1, 19, 31, and 40. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

I. Rejections Under 35 U.S.C. §101

The Office Action indicates that claims 1 – 18 and 31 – 46 stand rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter. Applicants amend claims 1, 31, and 40, as indicated above. Accordingly, Applicants consider this issue moot for claims 1 – 13, and 31 – 46.

With regard to claims 14 – 18, Applicants respectfully traverse this rejection for at least the reason that these claims include "means for" language that invokes 35 U.S.C. §112 ¶6. As "means for" claims are a statutorily recognized claim, Applicants submit that these claims, in their current format, meet all the requirements of 35 U.S.C. §101. As additional proof, MPEP §2181 states (quoting *In re Donaldson Co.*, 16 F.3d 1189, 1195, 29 USPQ2d 1845, 1850 (Fed. Cir. 1994) (in banc)) "35 U.S.C. 112, sixth paragraph states that a claim limitation expressed in means-plus-function language "shall be construed to cover the corresponding structure" (emphasis added). Accordingly, Applicants submit that this rejection is improper and that claims 14 – 18 meet all the requirements of 35 U.S.C. §101.

II. Rejections Under 35 U.S.C. §102

A. Claim 1 is Allowable Over *Thompson*

The Office Action indicates that claim 1 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent 1,111,495 A1 ("*Thompson*"). Applicants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 1 recites:

> A computer security system, comprising:
> a processor; and
> a memory component that stores:
> a security module adapted to control access to a secure computer resource by a user via a client based on verification of a security credential provided by the user; and
> verification data disposed on the client and accessible by the security module, the security module adapted to enable the user to ***recover the security credential from the client based*** on a response received from the user associated with the verification data.

(Emphasis added).

Applicants respectfully submit that claim 1 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security system, comprising… a memory component that stores… verification data disposed on the client and accessible by the security module, the security module adapted to enable the user to ***recover the security credential from the client based*** on a response received from the user associated with the verification data" as recited in claim 1. More specifically, *Thompson* discloses:

> When the PC is booted, the security program executes first and prompts the user for a password… and compares it with the stored password. If the passwords to not match, boot is aborted and the PC is disabled… The encrypted password is also registered with a remote trusted certificate authority (TCA 150). To establish or change the password a communication connection is established from the PC to the TCA or storage device.

(Abstract).

As illustrated in this passage, *Thompson* appears to disclose utilizing, during boot, a local password to continue the boot and access at least one computer application. The TCA

appears to include a remote device utilized to update and/or establish the password. Nowhere, however, is there any suggestion of "verification data disposed on the client and accessible by the security module, the security module adapted to enable the user to ***recover the security credential from the client based*** on a response received from the user associated with the verification data" as recited in claim 1.

Additionally, while the Office Action refers to FIG. 4, elements 404 – 418 to reject this portion of claim 1, Applicants respectfully disagree with this analysis. More specifically, referring to FIG. 4, *Thompson* discloses "CPU 102 encrypts the received password... and then compares the encrypted received password with password 306... to determine if they match. If they do not match, CPU102 halts the boot and further operation of PC 100, at step 410, rendering PC 100 unusable" (column 6, beginning line 8). As illustrated in this passage and FIG. 4, if the received password is incorrect, the process simply halts (FIG. 4, 410) with no other action being taken. There is absolutely no suggestion of recovering the password. For at least the reason that *Thompson* fails to even suggest this element of claim 1, claim 1 is allowable.

B. Claim 14 is Allowable Over *Thompson*

The Office Action indicates that claim 14 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent 1,111,495 A1 ("*Thompson*"). Applicants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 14 recites:

> A computer security system, comprising:
> means for controlling access to a secure computer resource associated with a client based on verification of a security credential provided by a user of the client; and
> means for accessing verification data disposed on the client to enable the user to ***recover the security credential*** based on a response received from the user via the controlling means.

(Emphasis added).

Applicants respectfully submit that claim 14 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security system, comprising… means for accessing verification data disposed on the client to enable the user to ***recover the security credential*** based on a response received from the user via the controlling means" as recited in claim 14. More specifically, *Thompson* discloses:

> When the PC is booted, the security program executes first and prompts the user for a password… and compares it with the stored password. If the passwords to not match, boot is aborted and the PC is disabled… The encrypted password is also registered with a remote trusted certificate authority (TCA 150). To establish or change the password a communication connection is established from the PC to the TCA or storage device.

(Abstract).

As illustrated in this passage, *Thompson* appears to disclose utilizing, during boot, a local password to continue the boot and access at least one computer application. The TCA appears to include a remote device utilized to update and/or establish the password. Nowhere, however, is there any suggestion of "means for accessing verification data disposed on the client to enable the user to ***recover the security credential*** based on a response received from the user via the controlling means" as recited in claim 14.

Additionally, while the Office Action refers to FIG. 4, elements 404 – 418 to reject this portion of claim 14, Applicants respectfully disagree with this analysis. More specifically, referring to FIG. 4, *Thompson* discloses "CPU 102 encrypts the received password… and then compares the encrypted received password with password 306… to determine if they match. If they do not match, CPU102 halts the boot and further operation of PC 100, at step 410, rendering PC 100 unusable" (column 6, beginning line 8). As illustrated in this passage and FIG. 4, if the received password is incorrect, the process simply halts (FIG. 4, 410) with no other action being taken. There is absolutely no suggestion of recovering the password. For at least the reason that *Thompson* fails to even suggest this element of claim 14, claim 14 is allowable.

C. **Claim 19 is Allowable Over *Thompson***

The Office Action indicates that claim 19 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent 1,111,495 A1 ("*Thompson*"). Applicants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 19 recites:

> A computer security method, comprising:
> receiving a request at a client to access a secure computer resource, a security credential required from a user to access the secure computer resource;
> presenting verification data disposed on the client to the user; and
> enabling the user to ***recover the security credential from the client*** based on a response received from the user to the verification data.
> ***(Emphasis added).***

Applicants respectfully submit that claim 19 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security method, comprising… enabling the user to ***recover the security credential from the client*** based on a response received from the user to the verification data" as recited in claim 19. More specifically, *Thompson* discloses:

> When the PC is booted, the security program executes first and prompts the user for a password… and compares it with the stored password. If the passwords to not match, boot is aborted and the PC is disabled… The encrypted password is also registered with a remote trusted certificate authority (TCA 150). To establish or change the password a communication connection is established from the PC to the TCA or storage device.
> (Abstract).

As illustrated in this passage, *Thompson* appears to disclose utilizing, during boot, a local password to continue the boot and access at least one computer application. The TCA appears to include a remote device utilized to update and/or establish the password. Nowhere, however, is there any suggestion of "enabling the user to ***recover the security credential from the client*** based on a response received from the user to the verification data" as recited in claim 19.

Additionally, while the Office Action refers to FIG. 4, elements 404 – 418 to reject this portion of claim 19, Applicants respectfully disagree with this analysis. More specifically, referring to FIG. 4, *Thompson* discloses "CPU 102 encrypts the received password… and then compares the encrypted received password with password 306… to determine if they match. If they do not match, CPU102 halts the boot and further operation of PC 100, at step 410, rendering PC 100 unusable" (column 6, beginning line 8). As illustrated in this passage and FIG. 4, if the received password is incorrect, the process simply halts (FIG. 4, 410) with no other action being taken. There is absolutely no suggestion of recovering the password. For at least the reason that *Thompson* fails to even suggest this element of claim 19, claim 19 is allowable.

D. Claim 31 is Allowable Over *Thompson*

The Office Action indicates that claim 31 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent 1,111,495 A1 ("*Thompson*"). Applicants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 31 recites:

> A computer security system, comprising:
> a processor; and
> a memory component that stores:
> a collection module adapted to receive and store verification data associated with a user on a client; and
> a recovery module adapted to enable the user to ***recover from the client a security credential associated with accessing a secure computer resource*** via the client by verifying the user response to the verification data.
> ***(Emphasis added).***

Applicants respectfully submit that claim 31 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security system, comprising… a recovery module adapted to enable the user to ***recover from the client a security credential associated with accessing a secure computer resource*** via the client by

verifying the user response to the verification data" as recited in claim 31. More specifically, *Thompson* discloses:

> When the PC is booted, the security program executes first and prompts the user for a password… and compares it with the stored password. If the passwords to not match, boot is aborted and the PC is disabled… The encrypted password is also registered with a remote trusted certificate authority (TCA 150). To establish or change the password a communication connection is established from the PC to the TCA or storage device. (Abstract).

As illustrated in this passage, *Thompson* appears to disclose utilizing, during boot, a local password to continue the boot and access at least one computer application. The TCA appears to include a remote device utilized to update and/or establish the password. Nowhere, however, is there any suggestion of "a recovery module adapted to enable the user to ***recover from the client a security credential associated with accessing a secure computer resource*** via the client by verifying the user response to the verification data" as recited in claim 31.

Additionally, while the Office Action refers to FIG. 4, elements 404 – 418 to reject this portion of claim 31, Applicants respectfully disagree with this analysis. More specifically, referring to FIG. 4, *Thompson* discloses "CPU 102 encrypts the received password… and then compares the encrypted received password with password 306… to determine if they match. If they do not match, CPU102 halts the boot and further operation of PC 100, at step 410, rendering PC 100 unusable" (column 6, beginning line 8). As illustrated in this passage and FIG. 4, if the received password is incorrect, the process simply halts (FIG. 4, 410) with no other action being taken. There is absolutely no suggestion of recovering the password. For at least the reason that *Thompson* fails to even suggest this element of claim 31, claim 31 is allowable.

E. Claim 40 is Allowable Over *Thompson*

The Office Action indicates that claim 40 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent 1,111,495 A1 ("*Thompson*"). Applicants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 40 recites:

> A computing device, comprising:
> a processor; and
> a memory component that stores:
> a security module disposed on the computing device and configured to control access to a secure computer resource associated with the computing device based on authentication of a security credential; and
> a recovery module disposed on the computing device and configured to enable a user to ***retrieve the security credential from the computing device using verification data disposed on the computing device without accessing a resource external to the computer device***.
> ***(Emphasis added).***

Applicants respectfully submit that claim 40 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computing device, comprising… a memory component that stores… a recovery module disposed on the computing device and configured to enable a user to ***retrieve the security credential from the computing device using verification data disposed on the computing device without accessing a resource external to the computer device***" as recited in claim 40. More specifically, *Thompson* discloses:

> When the PC is booted, the security program executes first and prompts the user for a password… and compares it with the stored password. If the passwords to not match, boot is aborted and the PC is disabled… The encrypted password is also registered with a remote trusted certificate authority (TCA 150). To establish or change the password a communication connection is established from the PC to the TCA or storage device.
> (Abstract).

As illustrated in this passage, *Thompson* appears to disclose utilizing, during boot, a local password to continue the boot and access at least one computer application. The TCA appears to include a remote device utilized to update and/or establish the password. Nowhere, however, is there any suggestion of "a recovery module disposed on the computing device and configured to enable a user to ***retrieve the security credential from the computing device using verification data disposed on the computing device without accessing a resource external to the computer device***" as recited in claim 40.

Additionally, while the Office Action refers to FIG. 4, elements 404 – 418 to reject this portion of claim 40, Applicants respectfully disagree with this analysis. More specifically, referring to FIG. 4, *Thompson* discloses "CPU 102 encrypts the received password... and then compares the encrypted received password with password 306... to determine if they match. If they do not match, CPU102 halts the boot and further operation of PC 100, at step 410, rendering PC 100 unusable" (column 6, beginning line 8). As illustrated in this passage and FIG. 4, if the received password is incorrect, the process simply halts (FIG. 4, 410) with no other action being taken. There is absolutely no suggestion of recovering the password. For at least the reason that *Thompson* fails to even suggest this element of claim 40, claim 40 is allowable.

F. **Claims 2 – 13, 15 – 18, 20 – 30, 32 – 39, and 41 – 46 are Allowable Over *Thompson***

The Office Action indicates that claims 2 – 13, 15 – 18, 20 – 30, 32 – 39, and 41 – 46 stand rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent 1,111,495 A1 ("*Thompson*"). Applicants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, dependent claims 2 – 13 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 1. Dependent claims 15 – 18 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 14. Dependent claims 20 – 30 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 19. Dependent claims 32 – 39 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 31. Dependent claims 41 – 46 are believed to be allowable for at least the reason that these claims depend from allowable independent claim 40. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

CONCLUSION

In light of the foregoing amendments and for at least the reasons set forth above, Applicants respectfully submit that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the now pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested.

Any other statements in the Office Action that are not explicitly addressed herein are not intended to be admitted. In addition, any and all findings of inherency are traversed as not having been shown to be necessarily present. Furthermore, any and all findings of well-known art and Official Notice, or statements interpreted similarly, should not be considered well-known for the particular and specific reasons that the claimed combinations are too complex to support such conclusions and because the Office Action does not include specific findings predicated on sound technical and scientific reasoning to support such conclusions.

If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,

/afb/
Anthony F. Bonner Jr. Reg. No. 55,012

THOMAS, KAYDEN,
HORSTEMEYER & RISLEY, L.L.P.
Suite 1500
600 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500